Hacker Highschool
SECURITY AWARENESS FOR TEENS



LECCIÓN 3
PUERTOS Y PROTOCOLOS









"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto.

El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a esponsorizarlo a través de la compra de una licencia, una donación o una esponsorización.

All works copyright ISECOM, 2004.





Índice





Contribuciones

Gary Axten, ISECOM

La Salle URL Barcelona

Kim Truett, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Pete Herzog, ISECOM









3.1. Objetivos

En la presente lección se parte de unos conocimientos básicos sobre Windows y Linux, para luego aplicarlos a los conocimientos sobre qué son y para qué sirven los puertos y protocolos.

Al término de la lección el alumno debe tener unos conocimientos básicos sobre:

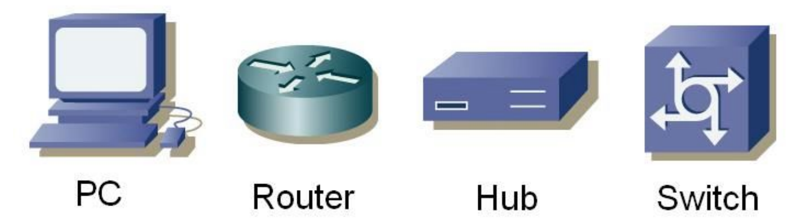
- Conceptos básicos de redes.
- Direccionamiento IP.
- Puertos y Protocolos.



3.2. Conceptos básicos de redes

3.2.1 Dispositivos

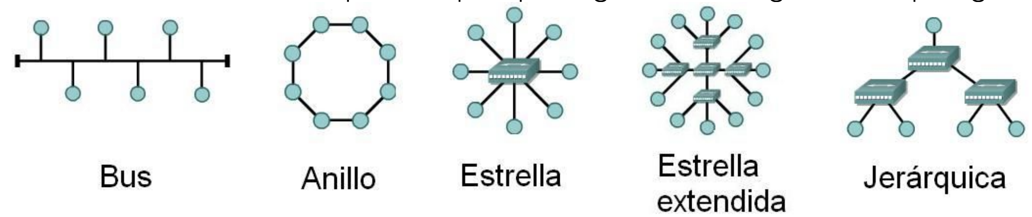
Antes de empezar a explicar protocolos y puertos, hay que familiarizarse con los iconos de los dispositivos más comunes que se ven en los esquemas básicos. Éstos son:



3.2.2 Topologías

Con estos dispositivos se pueden crear las denominadas redes de área local o LAN (Local Area Network). Con una LAN se puede tener una comunicación eficaz de dispositivos tales como ordenadores e impresoras para compartir recursos, se puede dar acceso a Internet con total control del administrador, etc.

A la hora de diseñar una LAN, se puede optar por alguna de las siguientes topologías físicas:



En la primera, topología de *Bus*, se tienen todos los ordenadores conectados a un único medio de transmisión que a su vez está conectado a unas terminaciones a ambos lados. Todos los ordenadores se ven entre sí.

En la configuración en *Anillo* se conecta un ordenador al siguiente, y el último al primero, de esta manera sólo se ve un ordenador con el contiguo.

En la topología en *Estrella* se conectan todos los terminales a un único punto central y es éste el que se encarga de retransmitir la información. Si se conectan varios puntos centrales entre sí, se obtiene una topología de *Estrella Extendida*.

Por lo contrario, si se van concatenando dispositivos a diferentes niveles se obtiene una topología *Jerárquica*.





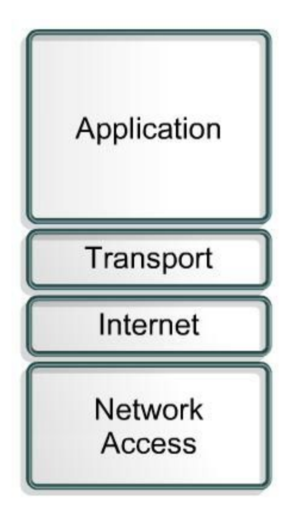
3.3. Modelo TCP/IP

3.3.1 Introducción

El modelo TCP/IP fue desarrollado por el DoD (Department of Defense) de los EUA y DARPA (Defense Advanced Research Project Agency) en la década de los 70. El modelo TCP/IP fue pensado como un estándar abierto para poder conectar dos máquinas cualesquiera, todo el mundo puede utilizarlo y es en el que se basa Internet.

3.3.2 Capas TCP/IP

El modelo TCP/IP define cuatro capas totalmente independientes en las que divide el proceso de comunicación entre dos dispositivos. Las capas por las que pasa la información entre dos estaciones o máquinas son las siguientes:



3.3.2.1 Aplicación

Es la capa más cercana al usuario final y la que le proporciona servicios de red. Como es la capa superior, no da servicios a ninguna capa. Es la responsable de traducir los datos de la aplicación, programa, para que puedan ser enviados por la red. Sus funciones se resumen en:

- Representación
- Codificación
- Control de diálogo
- Gestión de las aplicaciones de usuario

3.3.2.2 Transporte

La capa de transporte establece, mantiene y termina circuitos virtuales, proporciona mecanismos de control de flujo y permite las retransmisiones y proporciona mecanismos de detección y corrección de errores. La información que le llega de la capa de aplicación la divide formando diferentes segmentos. El direccionamiento se realiza a través de puertos. Sus funcionalidades básicas son:





- Fiabilidad
- Control de flujo
- Corrección de errores
- Retransmisión

3.3.2.3 IP

Divide los segmentos de la capa de transporte en paquetes y los envía por la red. No proporciona fiabilidad en las conexiones, de esto ya se ocupa la capa de transporte. Realiza un direccionamiento lógico de red mediante las direcciones IP.

Es la capa responsable de proporcionar conectividad entre usuarios. Selecciona la mejor ruta a elegir entre origen y destino.

3.3.2.4 Acceso a Red

Se encarga de controlar el acceso al nivel físico utilizado y enviar la información por el mismo. Transforma a información básica (bits) toda la información que le llega de las capas superiores y la prepara para que se pueda enviar por el medio. El direccionamiento físico de la red lo hace mediante direcciones MAC.

3.3.3 Protocolos

Para poder enviar información entre dos máquinas, es necesario que ambas estaciones hablen el mismo lenguaje para que se entiendan entre ellas. A este lenguaje se le llamará *protocolo*.

Los protocolos más representativos que figuran en la capa de Aplicación de la torre TCP/IP son:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Trivial File Transfer Protocol (TFTP)

Los protocolos de la capa de Transporte son:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

El protocolo más conocido de la capa de Internet es:

- Internet Protocol (IP)

El protocolo utilizado en la mayoría de redes locales en la capa de Acceso es:

- Ethernet

A continuación se describirán los protocolos anteriormente comentados y su puerto asociado de la capa de Transporte. Más adelante se detallarán todos los puertos y su significado.





3.3.3.1 Protocolos de la capa de Aplicación

El protocolo FTP es útil para la transmisión de archivos entre dos máquinas. Utiliza TCP para crear una conexión virtual para la información de control, y luego crea otra conexión para el envío de datos. Los puertos utilizados son el puerto 20 y 21.

El protocolo HTTP es para visualizar la mayoría de páginas web de Internet. Sus mensajes se distribuyen como los de correo electrónico. El puerto que se utiliza es el 80.

El protocolo SMTP es un servicio de correo que se basa en el modelo de FTP. Transfiere mensajes de correo entre dos sistemas y provee de notificaciones de correo entrante. El puerto que se utiliza es el 25.

El protocolo DNS es el que se encarga de reconocer el nombre de la máquina remota con la que se quiere establecer la conexión y traduce el nombre a su dirección IP. El puerto que se utiliza es el 53.

El protocolo TFTP tiene las mismas funciones que el protocolo FTP pero funciona sobre UDP, con lo que hay mayor rapidez pero menor seguridad y confiabilidad. El puerto que se utiliza es el 69.

3.3.3.2 Protocolos de la capa de Transporte

Dentro de la capa de transporte existen dos protocolos que se utilizan para el envío de segmentos de información:

- TCP: El protocolo TCP establece una conexión lógica entre puntos finales de la red. Sincroniza y regula el tráfico con lo que se conoce como "Three Way Handshake". Controla el flujo para que no se pierdan los paquetes y evitar así una congestión en la red. Es un protocolo orientado a conexión.
- UDP: El protocolo UDP es un protocolo de transporte no orientado a conexión que intercambia datagramas sin la utilización de ACK ni SYN que se utiliza como acuse de recibo en el caso de TCP. El procesamiento de errores y retransmisiones es soportado por los protocolos de capas superiores.

3.3.3.3 Protocolos de la capa de Internet

El protocolo IP sirve como protocolo universal para unir dos ordenadores en cualquier momento, lugar y tiempo.

No es un protocolo orientado a conexión y no es confiable.

Ofrece servicios de Best Effort: hará cuanto sea posible para que funcione correctamente.

El protocolo IP determina el formato de la cabecera del paquete IP donde se incluye la dirección lógica y otras informaciones de control.

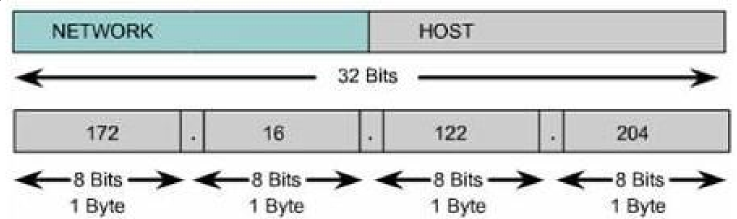
3.3.4 Direcciones IP

Las direcciones IP son los identificadores que se utilizan para diferenciar a cualquier dispositivo que se encuentre en la red. Cada dispositivo debe tener una dirección IP diferente para que no haya problemas de identidad dentro de la red.





La dirección IP consta de 32 bits que se dividen en 4 octetos (8 bits) separándolos por puntos. Lógicamente se compone de una parte que identifica la dirección de red (network) a la que pertenece y una segunda parte que es su propio identificador dentro de esa red, dirección de máquina (host).



Hay direcciones IP públicas y privadas. Las primeras deben ser únicas en todo Internet porque sino no sería posible el encaminamiento y por tanto la comunicación. En cambio, las direcciones privadas corresponden a redes de uso privado y que no tienen conexión alguna con otras redes, no tienen conexión a Internet. En las redes privadas hay que tener en cuenta que no se puede duplicar ninguna dirección IP en toda la red privada.

Las direcciones IP privadas existentes y que están definidas por el organismo internacional IANA son las que se engloban en los márgenes siguientes:

10.0.0.0 a 10.255.255.255
172.16.0.0 a 172.31.255.255
192.168.0.0. a 192.168.255.255

Las direcciones IP se dividen en clases que dependen del tamaño asignado para la parte de red y el tamaño que corresponde a la parte de la máquina.

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Según el tamaño asignado a cada parte se podrán o crear más redes o albergar más dispositivos en cada red creada. Las clases existentes son:

- Clase A: El primer bit es siempre cero, con lo que comprende las direcciones entre 0.0.0.0 a 126.255.255.255. Las direcciones de 127.x.x.x están reservadas para el servicio de *loopback* o *localhost*.
- Clase B: Los dos primeros bits del primer octeto son '10'. Las direcciones que pertenecen a esta clase están comprendidas entre 128.0.0.0 y 191.255.255.255.





- Clase C: Los tres primeros bits del primer octeto son '110'. Las direcciones están comprendidas entre 192.0.0.0 y 223.255.255.255.
- Clase D: Los cuatro primeros bits del primer octeto son '1110'. Las direcciones están comprendidas entre 224.0.0.0 y 239.255.255.255. Se utilizan para grupos *multicast*. Las restantes direcciones son para experimentación. A este último grupo se les puede encontrar como Clase E.

Actualmente, para la diferenciación entre la parte de red y la parte de máquina no se utilizan las clases, sino que lo que se utiliza es la máscara.

La máscara identifica con un '1' binario la parte que es de red y con un '0' binario la parte que es de máquina. Por lo tanto, para identificar una máquina, además de la dirección IP es necesario especificar una máscara de red:

IP: 172.16.1.20
Máscara: 255.255.255.0

Se ha visto que las direcciones IP 127.X.X.X estaban reservadas y que no se pueden utilizar para identificar a ningún dispositivo. Del mismo modo existen otras direcciones de máquina que no se pueden utilizar, éstas son la dirección de red y la dirección de braodcast.

La dirección de red es aquella en que la parte que identifica al dispositivo dentro de la red es toda ceros. Esta dirección no se puede utilizar ya que identifica a una red y, por lo tanto, nunca debe identificar a un dispositivo en concreto.

IP: 172.16.1.0
Máscara: 255.255.255.0

La dirección de bradcast es aquella que los bits que identifican al dispositivo dentro de la red son todo unos. Esta dirección tampoco se puede usar ya que es la que se utiliza cuando se quiere enviar alguna información a todas las máquinas que pertenecen a una red en concreto.

IP: 172.16.1.255
Máscara: 255.255.255.0

3.3.5 Puertos

Tanto TCP como UDP utilizan puertos para pasarse información con las capas superiores. Con la definición de un puerto, es posible acceder a un mismo destino, un host, y aplicar sobre él distintos servicios.

Con la utilización de los puertos los servidores son capaces de saber qué tipo de petición a nivel de aplicación le están solicitando, si es http o ftp, y pueden mantener más de una comunicación simultánea con diferentes clientes.





Si se quiere acceder a la web de www.osstmm.org cuya IP es 62.80.122.203, como el servidor de WEB está en el puerto 80, lo que se está estableciendo es una conexión al denominado socket

62.80.122.203:80

Para entenderlo mejor, se puede hacer la analogía siguiente: pensemos que la dirección IP es como el puerto de Barcelona, donde llegan muchos barcos, y los puertos de las direcciones IP son cada uno de los muelles en los que van a parar cada barco.

Para poder mantener una coherencia en los números de los puertos la IANA, organismo internacional regulador, establece que los puertos inferiores a 1024 se utilizan para los servicios comunes y el resto de números de puertos es para asignaciones dinámicas de programas o servicios particulares.

A continuación se listan los puertos más utilizados:

Asignación de Puertos		
Valor	**Nombre**	**Descripción**
0		Reserved
1-4		Unassigned
5	rje	Remote Job Entry
7	echo	Echo
9	discard	Discard
11	systat	Active Users
13	daytime	Daytime
15	netstat	Who is Up or NETSTAT
17	qotd	Quote of the Day
19	chargen	Character Generator
20	ftp-data	File Transfer [Default Data]
21	ftp	File Transfer [Control]
22	ssh	SSH Remote Login Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transfer
37	time	Time
39	rlp	Resource Location Protocol
42	nameserver	Host Name Server
43	nicname	Who Is
53	domain	Domain Name Server
67	bootps	Bootstrap Protocol Server
68	bootpc	Bootstrap Protocol Client
69	tftp	Trivial File Transfer
70	gopher	Gopher
75		any private dial out service
77		any private RJE service
79	finger	Finger



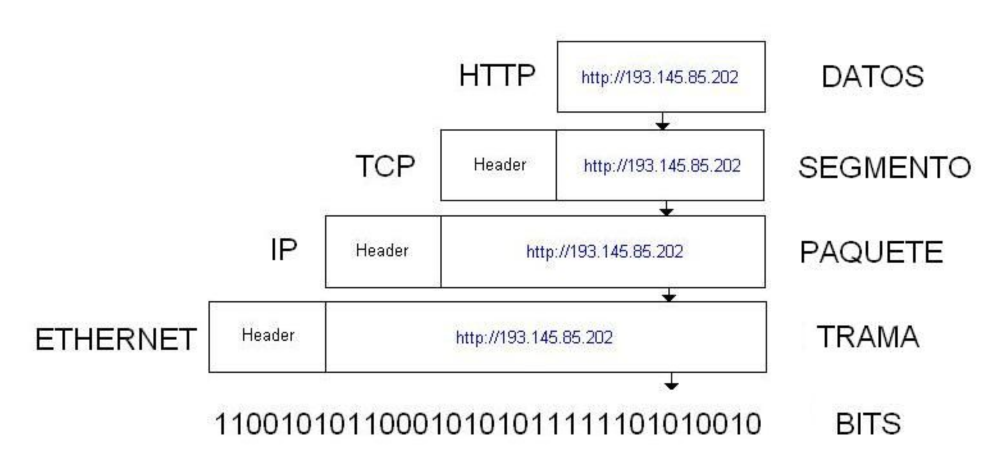


Asignación de Puertos		
Valor	**Nombre**	**Descripción**
80	www-http	World Wide Web HTTP
95	supdup	SUPDUP
101	hostname	NIC Host Name Server
102	iso-tsap	ISO-TSAP Class 0
110	pop3	Post Office Protocol - Version 3
113	auth	Authentication Service
117	uucp-path	UUCP Path Service
119	nntp	Network News Transfer Protocol
123	ntp	Network Time Protocol
137	netbios-ns	NETBIOS Name Service
138	netbios-dgm	NETBIOS Datagram Service
139	netbios-ssn	NETBIOS Session Service
140-159		Unassigned
160-223		Reserved

3.3.6 Encapsulación

Para enviar, por ejemplo, un mail desde un ordenador a otro la información irá pasando una serie de transformaciones, es decir, la capa superior generará una serie de datos que será recogida por la capa inmediatamente inferior. La capa inferior cogerá la información que le han pasado y le añadirá una cabecera para poder agregar información suficiente para que la capa del mismo nivel del destino pueda entender qué debe hacer con aquella información. A este procedimiento recursivo se le conoce con el nombre de *encapsulación*. Cada capa hace una encapsulación de la anterior, hasta llegar a la última capa, la de enlace, que hace posible la transmisión de los datos por el medio físico de la LAN: cable, radio, etc.

En el siguiente esquema se explica la encapsulación de una forma más gráfica:



Cuando la información encapsulada llega al destino, éste sólo tiene que desencapsular la información realizando el procedimiento contrario.





3.4. Ejercicios

3.4.1 Ejercicio 1: Netstat

El comando Netstat permite visualizar el estado de los puertos de un ordenador. Para poderlo ejecutar se tiene que abrir una ventana de MS-Dos y teclear:

netstat

En la salida por pantalla se pueden ver las conexiones actuales establecidas. Si se quiere que la salida esté en formato numérico se debe ejecutar:

netstat –n

Si lo que se desea es ver el estado tanto de las conexiones establecidas como de los puertos que están activos se debe ejecutar:

netstat –an

Para saber todas las opciones que se pueden añadir al comando netstat se puede ejecutar:

netstat -h

Se debe identificar qué puertos se usan de forma local y cuáles de forma remota. La segunda y la tercera columna determinan la dirección local y la remota.

¿Por qué los números de puertos remotos son diferentes a los números locales?

A continuación abrir el explorador con la página:

http://193.145.85.202
¿Qué conexión/conexiones nuevas aparecen?

Abrir otro explorador con la página:

http://193.145.85.203
Si se vuelve a ejecutar el comando netstat:

- ¿Por qué el protocolo http aparece en varias líneas?
- ¿Qué diferencias existen entre cada una de ellas?
- ¿Si hay varios exploradores abiertos como es el caso, cómo sabe para quién va la información de cada una de las páginas?
- ¿Necesita diferenciarla?
- Comenta la respuesta.

3.4.2 Ejercicio 2: Puertos y protocolos

Durante toda la lección se ha comentado que para diferenciar el servicio se usan diferentes puertos. ¿Cómo es que cuando se utiliza el navegador no se especifica ningún puerto?

¿Qué protocolos se utilizan?

¿Es posible que algún protocolo se utilice en más de una ocasión?





3.4.3 Ejercicio 3: Mi primer servidor

Para poder realizar este ejercicio primero es necesario conseguir el programa 'netcat' para windows. Se podrá conseguir si se accede a la página:

http://www.atstake.com/research/tools/network_utilities/

Una vez se haya conseguido el programa se debe descomprimir, abrir una ventana de MS-Dos, acceder al directorio donde se encuentre y teclear:

nc –h

Con esto se pueden ver las múltiples opciones que se pueden especificar en el netcat. Si se desea crear un pequeño servidor:

nc -l -p 1234

Al ejecutar este comando se está haciendo que se abra el puerto 1234 y se permitan conexiones entrantes. Seguidamente teclear desde otra ventana de MS-Dos:

netstat –a

Se comprueba que ha aparecido un nuevo servicio escuchando en el puerto 1234. Para salir del servidor, se puede utilizar: CTRL-C

Para poder decir que se ha implementado un servidor se necesita establecer el cliente asociado. Para ello se debe abrir una ventana de MS-Dos y, teniendo el servidor funcionando, ejecutar

nc localhost 1234

Con este comando se realizará una conexión hacia nuestro dispositivo utilizando el puerto 1234. Si ahora se escribe cualquier palabra en cualquiera de las dos ventanas de MS-Dos, tanto cliente como servidor, se verá como esa información se transmite hacia el otro.

Si se quiere que cada vez que se realice una conexión hacia el servidor se transmita al cliente cierta información, se deberá crear un fichero texto con la información que queramos transmitir, por ejemplo: "Bienvenido al servidor de Hacker High School". Una vez creado dicho fichero, con el nombre test, se deberá activar el servidor con el comando:

nc -l -p 1234 < test

Desde otra ventana de MS-Dos se intenta acceder al servidor:

nc localhost 1234

En el momento que se conecta se puede observar cómo en el cliente aparece el texto introducido en el fichero test. A partir de este punto la relación cliente/servidor es la misma que en el caso anterior.

¿Qué protocolo se ha usado para conectarte al servidor? ¿Permite netcat hacer lo mismo con otro protocolo?





3.5. Lecturas recomendadas

Si se desea tener más información sobre los temas que se han tratado en esta lección se pueden consultar los siguientes links, donde se ve de una forma más detallada toda la temática expuesta:

http://www.oreilly.com/catalog/fire2/chapter/ch13.html
http://www.oreilly.com/catalog/puis3/chapter/ch11.pdf
http://www.oreilly.com/catalog/ipv6ess/chapter/ch02.pdf
http://info.acm.org/crossroads/xrds1-1/tcpjmy.html
http://www.garykessler.net/library/tcpip.html
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm
http://www.redbooks.ibm.com/redbooks/GG243376.html